PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 1/00 — A2

(11) International Publication Number: WO 99/35554

(43) International Publication Date: 15 July 1999 (15.07.99)

(21) International Application Number: PCT/IB98/01969

(22) International Filing Date: 7 December 1998 (07.12.98)

(30) Priority Data:
09/000,668 30 December 1997 (30.12.97) US

(71) Applicant: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL–5621 BA Eindhoven (NL).

(71) Applicant *(for SE only)*: PHILIPS AB [SE/SE]; Kottbygatan 7, Kista, S–164 85 Stockholm (SE).

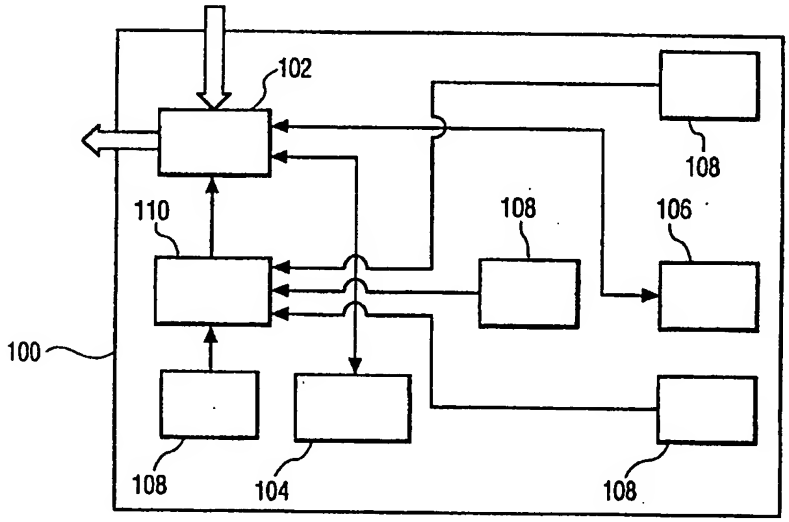
(72) Inventor: EPSTEIN, Michael, A.; Prof. Holstlaan 6, NL–5656 AA Eindhoven (US).

(74) Agent: KOPPEN, Jan; Internationaal Octrooibureau B.V., P.O. Box 220, NL–5600 AE Eindhoven (NL).

(81) Designated States: JP, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: METHOD AND APPARATUS FOR PROTECTION OF DATA ON AN INTEGRATED CIRCUIT BY USING MEMORY CELLS TO DETECT TAMPERING



(57) Abstract

Memory elements are physically distributed throughout a smart card. Each of these memory elements has a preset value or preset programmable value. Before release of information, the preset value of each memory element is checked to determine if the smart card has been tampered with by such methods as radiating or microwaving the card. If tampering is detected, information is barred from being released.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

Method and apparatus for protection of data on an integrated circuit by using memory cells to detect tampering.

A method and apparatus protects data on an integrated circuit to prevent disclosure of information from the card when an error or modification has been detected or reprogramming.

A smart card is a card similar in size to a typical credit card; however, it has a chip embedded in it. By adding a chip to the card, the smart card acquires power to serve many different uses including access-control and value exchange. A smart card may be used to store valuable information such as private keys, account numbers, passwords, or valuable personal information. Additionally, it permits performance of processes that are to be kept private, such as performing a public key or private key encryption.

An integrated circuit chip in the card typically allows protection of information being stored from damage or theft since, unlike magnetic stripe cards which carry information on the outside of the card, the information is internal. However, integrated circuits, particularly when used in smart cards, may allow release of information when an error is intentionally introduced through such methods as radiating or microwaving the smart card.

A smart card may generally include a processor such as an 8051 by Intel company for processing, a decrypter/encrypter using such technology as RSA, and a memory storing a key for use by the decrypter/encrypter although "memory cards" may include only memory.

A study by Bellcore has concluded that microwaving a smart card can produce a soft error in the decrypter/encrypter or memory as reported in "Smart Card Insecurity: Bellcore Advisory", IAC Newsletter DB, Sept. 30, 1996; Edge Publishing. By looking at the answer released by the smart card, one can analyze the released answer and based on that answer, determine the key stored in the memory, thus allowing access to private information.

The present invention provides a tampering check to prevent tampering of the integrated circuit. The present invention checks "canaries" such as registers, to determine if

they are "alive", i.e., producing a respective predetermined value. If the values from the "canaries" are not the respective predetermined values or comparison results are not as predetermined, information is not released from the smart card.

Figure 1 illustrates an example of a smart card including the present invention; and

Figure 2 illustrates an example of a smart card including a second embodiment invention.

Figure 1 illustrates a general layout of a smart card. Specifically, a smart card 100 may typically include cells such as a processor, for example, an Intel 8051 processor 102, a decrypter/encrypter using such technology as RSA 104, and a memory element storing a key such as a private key 106. Additionally, "canaries" or memory elements such as register elements, buffers, flip flops or memories such as SRAMS, E^2 cells 108 or other types of cells comparable to the cell concerned about being "hit" with radiation, etc., are physically distributed over the smart card to insure complete coverage and protection of the entire smart card.

The "canaries" should preferably be more sensitive than other cells so as to prevent corruption of only the "canaries" although "canaries" as sensitive as the other cells would also allow detection of tampering.

In one embodiment, the "canaries" are set to respective known states. The memory which holds the key, also holds reference values which are the same values as the respective known states. The known states can be the same value or different values for each of the "canaries" or a subset of the "canaries". The values can be prestored or can be calculated based on the key stored in the smart card memory.

When a user attempts to use the smart card and retrieve an output, a comparison is performed between each of the "canary" known states and their respective reference values stored in the memory.

A comparator present in the processor 102, or as a separate element 110, compares the state of the "canary" with the respective reference value for that "canary", producing a comparison result which is, if the comparator is a separate element, provided to the processor 102. The processor 102 takes the comparison result and using software, releases

the output or prevents release of the output. Alternatively, hardware 114 could be added to the output of the processor 102 to allow or prevent release of the output based on the comparison result. If the values match, output from the smart card is released externally. If the values do not match, the output is not released externally.

Additionally, often memory elements will "zero" (set all bits to zero) or "set" (set all bits to one) when one tampers with the integrated circuit. Thus, the comparator could check if each memory element is zeroed or set and bar release of information if either condition occurs.

Outputs from the "canaries" can also be compared against each other and checked that they are the same number, be added (or perform some other function) and compared to a prespecified number, or check that each is a prespecified number.

A known constant built into the comparator, should be of such quality that it is not affected by the radiation or other external influences. Indeed, any element providing a reference value or prespecified function, etc. should be of such quality that it is not affected by the radiation or other external influences.

Alternatively, the number of comparators may be varied or may be used in various combinations to insure that the smart card has not be affected by radiation or other tampering. One such example is shown in Figure 2.

Another alternative would have the canary outputs programmable with a preset pattern to randomize the output and protect against tampering.

As can now be readily appreciated, the invention allows detection of tampering of an integrated circuit. The invention may be included in a subsystem or may be a separate subsystem. One skilled in the art may easily use differing numbers of "canaries" or have each "canary" output more than one value. Additional modifications may easily be made by one skilled in the art.

Moreover, the present invention may be used on smart cards having only memory and no processor. The output of the canaries could be checked by a comparator in one of the methods or a method similar to those detailed above, and the output from the memory could be enabled or disabled based on the output of the comparator.

It will thus be seen that the objects set forth above among those made apparent from the preceding description, are efficiently attained and, since certain changes may be made in the above constructions without departing from the spirit and scope of the invention, it is intended that all matter contained in the above description or shown in the accompanying drawings shall be interpreted as illustrative and not limiting sense.

It is also to be understood that the following claims are intended to cover all of the generic and specific features of the invention herein described and all statements of the scope of the invention which, as a matter of language, might be said to fall therebetween.

CLAIMS:

1. A smart card comprising:

- a memory (106) storing a key;
- an encrypter/decrypter (104) for encrypting information supplied by the smart card and decrypting information received by the smart card using the key;
- a plurality of memory elements (108), each memory element (108) storing a respective preset value; and
- a comparator (110) for comparing the respective value of each memory element (108) with a reference value from said memory (106), said comparator (110) barring information from being supplied if any of the respective values of the memory elements (108) does not match the respective reference value.

2. A smart card comprising:

- a memory (106) storing information;
- at least one memory element (108), each memory element (108) storing a respective preset value; and
- at least one comparator (110) for comparing respective values of each memory element (108) in a preset manner to acquire at least one comparison result to produce an enabling signal, said enabling signal barring information from being supplied if any of the at least one comparison results does not match an at least one respective reference value.

3. A smart card as recited in Claim 2, wherein at least one of said at least one memory elements (108) is a programmable memory.

4. A method for preventing a smart card from providing information if the smart card has been tampered with, said method comprising the steps of:

- setting at least one memory element (108) to a preset value;
- comparing each respective set value of said at least one memory element (108) to a respective reference value;
- producing a comparison result based on said comparing; and

- enabling or disabling output of information from said smart card based on said comparison result.

1/1

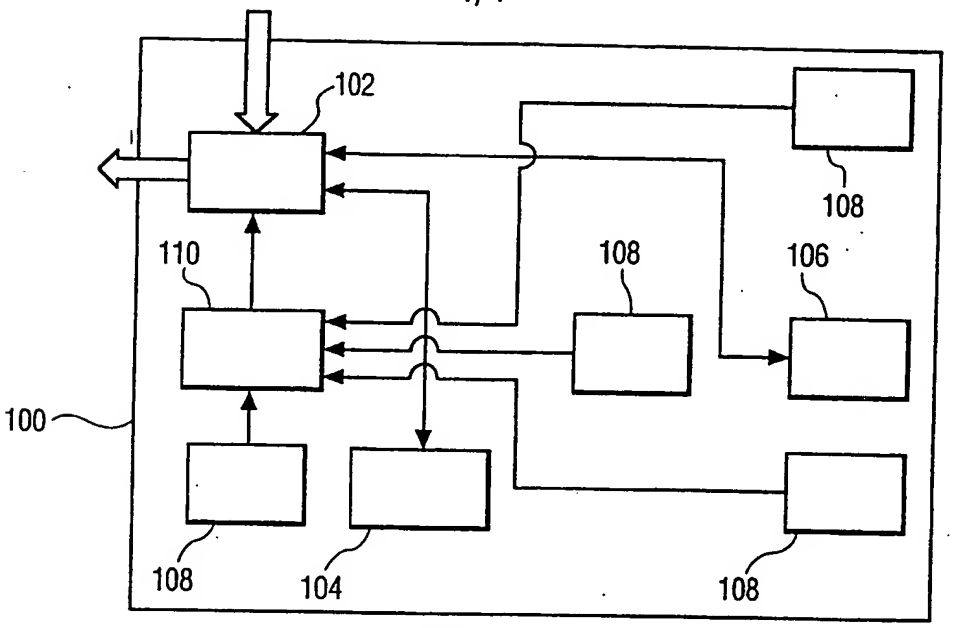

102
108
110
108
106
100
108
104
108

FIG. 1

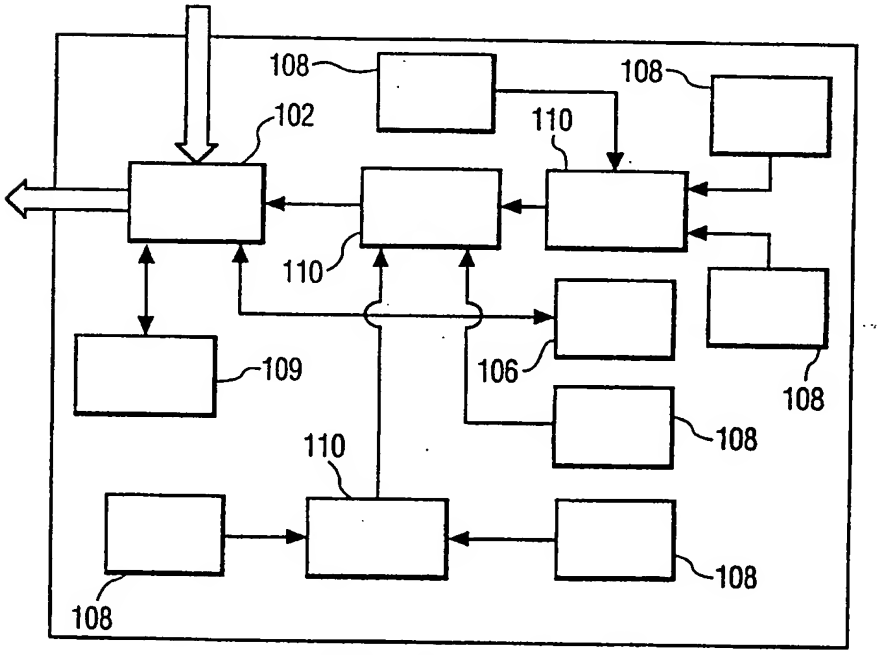

108
108
102
110
110
109
106
108
110
108
108

FIG. 2

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 1/00, G06K 19/073 — A3

(11) International Publication Number: **WO 99/35554**

(43) International Publication Date: 15 July 1999 (15.07.99)

(21) International Application Number: PCT/IB98/01969

(22) International Filing Date: 7 December 1998 (07.12.98)

(30) Priority Data:
09/000,668 30 December 1997 (30.12.97) US

(71) Applicant: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL–5621 BA Eindhoven (NL).

(71) Applicant *(for SE only)*: PHILIPS AB [SE/SE]; Kottbygatan 7, Kista, S–164 85 Stockholm (SE).

(72) Inventor: EPSTEIN, Michael, A.; Prof. Holstlaan 6, NL–5656 AA Eindhoven (US).

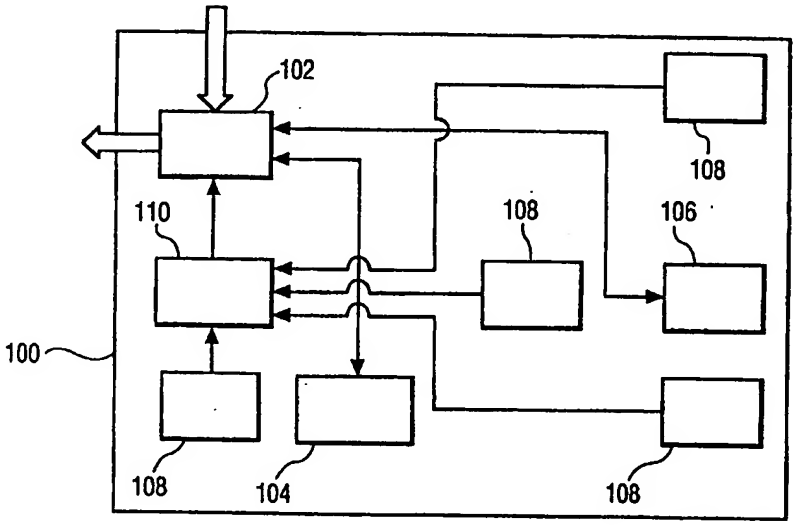
(74) Agent: KOPPEN, Jan; Internationaal Octrooibureau B.V., P.O. Box 220, NL–5600 AE Eindhoven (NL).

(81) Designated States: JP, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(88) Date of publication of the international search report:
16 September 1999 (16.09.99)

(54) Title: METHOD AND APPARATUS FOR PROTECTION OF DATA ON AN INTEGRATED CIRCUIT BY USING MEMORY CELLS TO DETECT TAMPERING



(57) Abstract

Memory elements are physically distributed throughout a smart card. Each of these memory elements has a preset value or preset programmable value. Before release of information, the preset value of each memory element is checked to determine if the smart card has been tampered with by such methods as radiating or microwaving the card. If tampering is detected, information is barred from being released.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB 98/01969

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: G06F 1/00, G06K 19/073
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: G06F, G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EDOC, WPIL, JAPIO

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5185717 A (RYOICHI MORI), 9 February 1993 (09.02.93), column 8, line 2 - column 10, line 40, figure 20 --	1-4
A	US 5237609 A (MASATOSHI KIMURA), 17 August 1993 (17.08.93), abstract --	1-4

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 June 1999	02 -07- 1999
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Bo Gustavsson/MN Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

01/06/99

International application No.
PCT/IB 98/01969

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5185717 A	09/02/93	US 5309387 A	03/05/94
		JP 2044447 A	14/02/90
		JP 2731912 B	25/03/98
US 5237609 A	17/08/93	FR 2645303 A,B	05/10/90
		GB 2233127 A,B	02/01/91
		JP 2259893 A	22/10/90
		JP 2677342 B	17/11/97
		JP 2259852 A	22/10/90
		JP 2507588 B	12/06/96